REMARKS/ARGUMENTS

The present Amendment is in response to the Office Action having a mailing date of December 13, 2005. Claims 1-22 are pending in the present Application. Applicant has amended claims 1, 5, 7, 13, and 16. Consequently, claims 1-22 remain pending in the present Application.

Applicant has amended the specification to more clearly indicate that the embedded security chip only allows cryptographic functions to be performed using this key if the system is bound. Support for the amendment can be found in the specification, 5, lines 19-21; page 6, lines 8-13; page 7, lines 9-14; and Figure 3. Applicant has amended claims 1, 7, and 16 to more clearly recite that the tag data indicates whether the key pair material is bound to the embedded security chip. Support for the amendment can be found in claims 1, 7, and 16 and in the specification, page 5, line 22-page 6, line 3. Applicant has also amended claims 1, 7, and 16 to recite that the tag data does not indicate the identity of the embedded security chip or the computer system. Support for the amendment can be found in the specification, page 6, lines 1-3 (indicating that the tag data may include a single bit that may be set or not depending upon the binding). Applicant has also amended claims 5 and 13 to recite encryption and user key pair levels. Support for the amendment can be found in the specification, page 6, lines 6-8.

In the above-identified Office Action, the Examiner rejected claims 2, 9, and 17 under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement. In particular, the Examiner cited the limitation that "binding is required for the key pair material" is not enabled by the specification. The Examiner noted that

> **[a]ccording to the specification . . . if the tag indicates that the key is a binding-required key, the embedded security chip only allows cryptographic functions to be performed using this key. If the tag indicates that the key is not designated as a binding required key, the embedded security chip allows all operations on the embedded security chip with that key regardless of binding. However, what constitutes <u>all operations</u> on the embedded security chip besides using only**

cryptographic functions to be performed is not specified and as such one skilled in the art clearly would not know how to make and use the same claimed invention to implement the case that the binding is required (or is not required) for the key pair material.

Applicant respectfully disagrees with the Examiner's rejection. Binding being required (or not required) is enabled by the specification. Applicant has amended the specification to more clearly indicate that for binding required keys, the embedded security chip only allows the embedded security chip only allows cryptographic functions to be performed using this key if the system is bound. However, for non-binding required keys, operations are allowed by the embedded security chip if the user is verified by their password. Specification, page 7, lines 1-5. For example, for binding required keys, "binding must be established with the system before platform key operations are enabled." Specification, page 6, lines 8-10. The specification also contrasts cases where binding is required (the key pair is bound to the system) and where binding is not required (key pair is not bound to the system). Specification, page 5, lines 19-21. See also, specification, page 6, lines 8-13. The specification also states:

> Accordingly, in a system and method in accordance with the present invention, the inclusion of tag data in the key material allows user keys to be designated as not binding-required, **so that they may be verified securely on any system**. Access to the embedded security subsystem remains secure, since the **platform is verified only on the system where binding is established**. In this manner, there is more selective allowance of key types based on binding.

Specification, page 7, lines 9-14 (emphasis added). As discussed throughout the specification, binding indicates whether the platform and the user must be verified. Consequently, Applicant respectfully submits that the term "binding is required for the key pair material" is enabled by the specification. Consequently, claims 2, 9, and 17 comply with the enablement requirement.

In the above-identified Office Action, the Examiner rejected claims 5 and 13 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and

distinctly claim the subject matter which applicant regards as the invention. The Examiner indicated that the claims indefinite because the claim language "the four levels further comprise a hardware key pair level, a platform key pair level, a user key pair level, and a credential key pair level" were not consistently defined in the specification. The Examiner noted that paragraph 19 indicates that level 1 is a platform key pair, level 2 includes key encrypting key pairs, and that level 3 key pairs are user keypairs.

Applicant respectfully traverses the Examiner's rejection. Applicant has amended claims 5 and 13 to recite the encryption and user key pairs. Applicant notes that user and credential key pairs were described in the background portion of the specification. See specification, page 3, lines 17-23 (paragraph 8). Although claims 5 and 13 have been amended to specify particular levels (hardware, platform, encryption and user), nothing prevents other claims for utilizing other levels. Because claims 5 and 13 recites the hardware, platform, encryption, and user key levels, Applicant respectfully submits that claims 5 and 13 are clear and definite.

In the above-identified Office Action, the Examiner also rejected claims 1, 7, and 16 under 35 U.S.C. § 103 as being unpatentable over U.S. Patent Application Publication No. 2003/0037237 (Abgrall) in view of U.S. Patent Application Publication No. 2003/0012383 (Bernsteinet). In so doing, the Examiner Abgrall, paragraphs 4, 105 and 191 as teaching creation of the key pair material for use with an embedded security chip. The Examiner also stated "however, Abgrall does not disclose expressly the key pair material including tag data. . ." Consequently, the Examiner relied upon Bernsteinet, paragraphs 5 and 10, as teaching determining whether the key pair material is bound based on tag data.

Applicant respectfully traverses the Examiner's rejection. Claims 1, 7, and 16 recite that the key pair material includes tag data, that the tag data indicates whether the key pair material is

bound to the embedded security chip without indicating an identity of the embedded security chip or the computer system and that it is determined whether the key pair material is bound to the embedded security chip based on the tag data without specifying the identity of the embedded security processor or the computer system. Consequently, key pair material can either be bound or may be used to verify a user securely on any system. Specification, page 7, lines 9-13.

Applicant agrees that the cited portions of Abgrall describe various aspects of security systems. Abgrall, paragraphs 4, 105, and 191. However, as the Examiner has acknowledged, Abgrall fails to disclose the use of tags in the key pair material. Consequently, Abgrall does not teach or suggest including with key pair material the tag data that indicates whether the key pair material is bound to the embedded security chip or determining whether the key pair is bound to the embedded security chip using the tag data.

Bernsteinet fails to remedy the defects of Abgrall. The cited portions of Bernsteinet describe the use of what amounts to a password. In particular, Bernsteinet describes the use of an "electronic footprint" that is "a unique or nearly enough unique value that is a combination of a selected set of identity information from the target desktop, selected from CPU, chipset and BIOS data, or the like and/or optionally the boot drive." Bernsteinet, paragraph 5. A single unique number is generated from the electronic footprint. Bernsteinet, paragraph 5. The electronic footprint is also used in an encryption sequence to provide a decryption key that allows only the system from which the electronic footprint is taken to decrypt associated software. Bernsteinet, paragraphs 6-7. Thus, although Bernsteinet describes a mechanism for validating software on a computer system, Applicant respectfully submits that Bernsteinet does so by providing a key that includes as part of it a number, which can be considered to correspond to a password, that is associated with the computer system. Consequently, Bernsteinet merely provides

a key for the computer system, rather than tag data used in determining whether key pair material is bound.

Because neither Bernsteinet nor Abgrall teach or suggest the recited tag data or using the tag data to determine whether key pair material is bound, any combination of Bernsteinet and Abgrall would also fail to teach or suggest this feature. Stated differently, if the cited portion of Bernsteinet were added to the teachings of Abgrall, the combination may be used to provide security based upon the "electronic footprint" of selected systems. In particular, the key used would include a representation of the electronic footprint that uniquely identifies the system. However, the combination would not be utilizing tag data to determine binding of the key pair material. Instead, the combination would effectively include a password uniquely representing the electronic system with which the software is used. Consequently, Abgrall in view of Bernsteinet fails to teach or suggest the methods and computer system recited in claims 1, 7, and 16.

In the above-identified Office Action, the Examiner also rejected claims 1-22 under 35 U.S.C. § 103 as being unpatentable over Abgrall in view of U.S. Patent No. 6,792,113 (Ansell).

Applicant respectfully traverses the Examiner's rejection. Independent claims 1, 7, and 16 all recite that the key pair material includes the tag data that indicates whether the key pair material is bound to the embedded security chip without indicating an identity of the embedded security chip or the computer system and determining whether the key pair is bound to the embedded security chip using the tag data. As discussed above, Abgrall fails to teach or suggest including with key pair material the tag data that indicates whether the key pair material is bound to the embedded security chip or determining whether the key pair is bound to the embedded security chip using the tag data.

Ansell fails to remedy the defects of Abgrall. Ansell describes a system that does allow a binding to a machine or to a user. Ansell, col. 2, lines 35-54. However, Ansell fails to teach or suggest a method or system in which key pair material includes tag data that is used in determining binding to an embedded security chip/security processor. Instead, Ansell utilizes passports. For machine binding, Ansell describes creating a passport that contains the private key for the machine and a public key for the machine. Ansell, col. 2, lines 35-38. The private key is based on a hardware identifier for the machine. Ansell, col. 2, lines 38-40. The public key is the reciprocal of the private key. Ansell, col. 2, lines 35-38. To this extent, Ansell is similar to Bernsteinet, which effectively uses a unique password corresponding to an individual computer system. Ansell also allows the creation of a passport for user binding. Such a passport also includes a private key and a public key that is the reciprocal of the private key. Ansell, col. 2, lines 54-64. However, the private key is based upon a password provided by the user. Ansell, col. 2, lines 56-60. Ansell further discloses changing the passport to machine binding for a passport for user binding. However, in order to do so, Ansell describes creating a *new* user passport using the keys of the machine-bound passport in conjunction with the user's password. Ansell, col. 3, lines 25-35.

Thus, it is the hardware identifier of Ansell that indicates that the keys are machine-bound. This hardware identifier is specific to a hardware device, for example a hash of the MAC address for the computer. Ansell, col. 6, lines 5-18. Similarly, it is the user password that indicates that the key is user-bound. Ansell, therefore, does not use tag data to determine whether the keys are user bound or machine bound. Instead, like Bernsteinet, Ansell utilizes quantities that are effectively passwords for the machine (the hardware identifier that is unique to a particular machine) and for the user (user password). Different passports have different passwords and, therefore, different keys depending in part on whether the keys are bound to a particular machine or user bound. For

example, the data indicating that a key is machine bound varies from machine to machine because the hardware identifier varies between machines. Consequently, in the system of Ansell utilizes passwords to determine whether particular keys for a particular passport are bound to a user or bound to a particular machine. Applicant respectfully submits that one of ordinary skill in the art would recognize that using different passwords for different types of binding and different passwords for machine binding to different types of machines are distinct from the recited tag data. Thus, Ansell fails to teach or suggest the recited tag data that is used to determine the binding of the key pair.

Because neither Ansell nor Abgrall teach or suggest the recited tag data or using the tag data to determine whether key pair material is bound, any combination of Ansell and Abgrall would also fail to teach or suggest this feature. Stated differently, if the cited portion of Ansell were added to the teachings of Abgrall, the combination may be used to provide security based upon the passports containing passwords corresponding either to a particular machine or to a particular user. In particular, the key used would include a representation of the electronic footprint that uniquely identifies the system. However, the combination would not be utilizing tag data to determine binding of the key pair material. Instead, the combination would effectively include a password uniquely representing the electronic system with which the software is used. Consequently, Abgrall in view of Ansell fails to teach or suggest the methods and computer system recited in claims 1, 7, and 16.

Claims 2-6, 8-15, and 17-22 depend upon independent claims 1, 7, and 16, respectively. Consequently, the arguments herein apply with full force to claims 2-6, 8-15, and 17-22. Accordingly, Applicant respectfully submits that claims 2-6, 8-15, and 17-22 are allowable over the cited references.

Claims 2, 9, and 17 are separately allowable over the cited references. Claims 2, 9, and 17 recite that the tag data further includes a bit that indicates whether binding is required for the key pair material. As discussed above, Ansell and Bernsteinet include an identifier specific to the computer system. Consequently, neither Ansell nor Bernsteinet teach or suggest the use of a single bit that indicates whether binding is required for the key pair material. Moreover, as discussed above, Abgrall fails to teach or suggest the use of the recited tag data. Consequently, Abgrall in view of Ansell or Bernsteinet fail to teach or suggest the methods and computer system recited in claims 2, 9, and 17. Accordingly, Applicant respectfully submits that claims 2, 9 and 17 are separately allowable over the cited references.

Applicant's attorney believes that this application is in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicant's attorney at the telephone number indicated below.

Respectfully submitted,

SAWYER LAW GROUP LLP

March 22, 2006
Date

/Janyce R. Mitchell/ Reg. No. 40,095
Janyce R. Mitchell
Attorney for Applicant(s)
(650) 493-4540